EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	37	((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and (prime adj number) and ((private symmetric) adj key)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:02
L2	1	10/566504	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 08:56
L3	16	((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and (public adj exponent) and ((crypto$5 secure security encryption private public) near2 (algorithm function))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:22
L4	1	((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and (public adj exponent) and ((modular adj product) with (private symmetric) adj (key))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:01
L5	1	((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((modular adj product) with (private symmetric) adj (key))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:02
L6	1	((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((modular adj product) same (private symmetric) adj (key))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:22
L7	1	((modular adj product) same (private symmetric) adj (key))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:02
L8	7	((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA")))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:12
L9	10	("20040215685"|"4736423"|"5991415"|"6144740"|"6965673").PN.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:14
L11	6	380/28-30,255,259.ccls. and (((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA"))))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:36

EAST Search History

L12	0	380/277,285.ccls. and (((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA"))))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:20
L13	1	380/44,46.ccls. and (((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA"))))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:20
L17	10	"708"/$.ccls. and (((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA"))))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:21
L18	5	"708"/492.ccls. and (((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA"))))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:21
L20	7	"708"/$.ccls. and ((euler adj totient) near2 (function algorithm method module calculat$3 determin$3))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:21
L21	1	(((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((modular adj product) same (private symmetric) adj (key))).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:22
L22	1	(((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and (public adj exponent) and ((crypto$5 secure security encryption private public) near2 (algorithm function))).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:22
L23	2	713/185,172.ccls. and (((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA"))))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:47
L24	0	726/9,20.ccls. and (((euler adj totient) near2 (function algorithm method module calculat$3 determin$3)) and ((private symmetric) adj key) and ((attack near2 (channel error "DPA" "SPA"))))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/11/13 09:47

Google Scholar BETA

Web Images Video News Maps more »

"euler totient" +DPA attack +crypto +RSA Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar

Results 1 - 6 of 6 for "euler totient" +DPA attack +crypto +RSA. (0.17 seconds)

All Results

S Yen
S Kim
S Lim
S Moon
L Batina

Tip: Try removing quotes from your search to get more results.

A countermeasure against one physical cryptanalysis may benefit another **attack** - all 4 versions »
SM Yen, S Kim, S Lim, S Moon - Information Security and Cryptology–ICISC, 2001 - Springer
... integer and φ(n) is the **Euler totient** function of ... is much more vulnerable to **DPA** than the ... A practical implementation of the timing **attack**," Technical Report ...
Cited by 24 - Related Articles - Web Search - BL Direct

A Side-channel **Attack** Resistant Programmable
N Mentens, K Sakiyama, L Batina, B Preneel, I ... - ieeexplore.ieee.org
... Using an SPA **attack** an adver ... To prevent Differential Power Analysis (**DPA**) attacks [11], [12], which ... of typically 20 bits) and o is the **Euler totient** function of ...
Web Search

[PDF] Side-Channel Analysis
M Joye, F Olivier - win.tue.nl
... r i and where φ denotes **Euler totient** function. ... editor, Advances in Cryptology – **CRYPTO** '99, volume ... order power analysis to **attack DPA** resistant software. ...
Related Articles - View as HTML - Web Search

Self-Randomized Exponentiation Algorithms - all 12 versions »
B Chevallier-Mames - Topics in Cryptology–CT-**RSA** - Springer
... This gave rise to fault **attacks** [BDL01] and ... C82] as the value of **Euler totient** function φ ... order to prevent Differential Power Analysis (**DPA**) [KJJ99], combining ...
Cited by 2 - Related Articles - Web Search - BL Direct

Hardware architectures for public key cryptography - all 6 versions »
L Batina, SB Ors, B Preneel, J Vandewalle - Integration, the VLSI Journal, 2003 - Elsevier
... We can say that **DPA** is more powerful than SPA but also is a "high ... The idea behind this type of **attack** is the fact that from time to time ... 3. **RSA** cryptosystem. ...
Cited by 38 - Related Articles - Web Search

[PDF] United States Patent (10) Patent No.: US 6,381,699 B2 - all 2 versions »
LR CRYPTOGRAPHIC - cryptography.com
... 3 shows an exemplary leak-resistant **RSA** private ... per operation for the given **attack**, 65 the ... proof (and, more generally, leak-resistant) **crypto**- systems provide ...
Related Articles - View as HTML - Web Search

"euler totient" +DPA attack +crypto + Search

Google Home - About Google - About Google Scholar

Tue, 13 Nov 2007, 9:27:33 AM EST

Edit an existing query or compose a new query in the Search Query Display.

Select a search number (#) to:

- Add a query to the Search Query Display
- Combine search queries using AND, OR, or NOT
- Delete a search
- Run a search

Search Query Display

[redacted]

Recent Search Queries

		Results
#1	(((euler totient)<in>metadata) <and> (private key<in>metadata))<and> (dpa<in>metadata)	0
#2	(((euler totient)<in>metadata) <and> (private key<in>metadata))	0
#3	(euler totient<in>metadata)	2
#4	(euler totient<in>metadata)	2
#5	((private key<in>metadata) <and> (dpa attack<in>metadata))<or> (spa attack<in>metadata)	1

[redacted]

Terms used: **euler totient DPA attack private key** Found **73** of **214,158**

Sort results by relevance Save results to a Binder Try an Advanced Search

Display results expanded form Search Tips Try this search in The ACM Guide

Open results in a new window

Results 1 - 20 of 73 Result page: **1** 2 3 4 next

Relevance scale

1 Digital circuits design: Current mask generation: a transistor level security against DPA attacks

Daniel Mesquita, Jean-Denis Techer, Lionel Torres, Gilles Sassatelli, Gaston Cambon, Michel Robert, Fernando Moraes

September 2005 **Proceedings of the 18th annual symposium on Integrated circuits and system design SBCCI '05**

Publisher: ACM Press

Full text available: pdf(513.86 KB) Additional Information: full citation, abstract, references, index terms

The physical implementation of cryptographic algorithms may leak to some attacker security information by the side channel data, as power consumption, timing, temperature or electromagnetic emanation. The Differential Power Analysis (DPA) is a powerful side channel attack, based only on the power consumption information. There are some countermeasures proposed at algorithmic or architectural level that are expensive and/or complexes. This paper addresses the DPA attack problem by a novel and eff ...

Keywords: DPA, countermeasures, cryptography, side channel attacks

2 Work-in-progress session on innovative topics: Security wrappers and power analysis for SoC technologies

C. H. Gebotys, Y. Zhang

October 2003 **Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '03**

Publisher: ACM Press

Full text available: pdf(790.57 KB) Additional Information: full citation, abstract, references, citings, index terms

Future wireless internet enabled devices will be increasingly powerful supporting many more applications including one of the most crucial, security. Although SoCs offer more resistance to bus probing attacks, power/EM attacks on cores and network snooping attacks by malicious code are relevant. This paper presents a methodology for security on NoC at both the network level (or transport layer) and at the core level (or application layer) is proposed. For the first time a low cost security wrapp ...

Keywords: VLIW, adiabatic, design, performance, security

3

Terms used: **euler totient DPA SPA private key** Found **31** of **214,158**

Sort results by relevance Save results to a Binder Try an Advanced Search

Display results expanded form Search Tips Try this search in The ACM Guide

Open results in a new window

Results 1 - 20 of 31 Result page: **1** 2 next

Relevance scale

1 Work-in-progress session on innovative topics: Security wrappers and power analysis for SoC technologies

C. H. Gebotys, Y. Zhang

October 2003 **Proceedings of the 1st IEEE/ACM/IFIP international conference on Hardware/software codesign and system synthesis CODES+ISSS '03**

Publisher: ACM Press

Full text available: pdf(790.57 KB) Additional Information: full citation, abstract, references, citings, index terms

Future wireless internet enabled devices will be increasingly powerful supporting many more applications including one of the most crucial, security. Although SoCs offer more resistance to bus probing attacks, power/EM attacks on cores and network snooping attacks by malicious code are relevant. This paper presents a methodology for security on NoC at both the network level (or transport layer) and at the core level (or application layer) is proposed. For the first time a low cost security wrapp ...

Keywords: VLIW, adiabatic, design, performance, security

2 Digital circuits design: Current mask generation: a transistor level security against DPA attacks

Daniel Mesquita, Jean-Denis Techer, Lionel Torres, Gilles Sassatelli, Gaston Cambon, Michel Robert, Fernando Moraes

September 2005 **Proceedings of the 18th annual symposium on Integrated circuits and system design SBCCI '05**

Publisher: ACM Press

Full text available: pdf(513.86 KB) Additional Information: full citation, abstract, references, index terms

The physical implementation of cryptographic algorithms may leak to some attacker security information by the side channel data, as power consumption, timing, temperature or electromagnetic emanation. The Differential Power Analysis (DPA) is a powerful side channel attack, based only on the power consumption information. There are some countermeasures proposed at algorithmic or architectural level that are expensive and/or complexes. This paper addresses the DPA attack problem by a novel and eff ...

Keywords: DPA, countermeasures, cryptography, side channel attacks

3